Claims

1. A data processing system for initially generating and installing at least one personal security device PSD master key replacement key and at least one PSD master key inside at least one PSD, said system comprising:

a first server including data storage means, wherein said first server is functionally connected to a first hardware security module HSM and a PSD writer;

said PSD writer functionally connected to said first server and said at least one PSD;

said at least one PSD including a non-mutable unique identification number, a security executive, a first high level key slot and a second high level key slot, wherein said PSD is functionally connected to said PSD writer;

said first HSM including at least one stored public key, at least one stored master key data block, at least one stored master key replacement key data block and means for generating random numbers, wherein said first HSM is functionally connected to said first server;

2. The system according to claim 1, wherein said non-mutable unique identification number is sent to said first HSM.

3. The system according to claim 1, wherein said first HSM comprises random number generating means for generating a random number.

4. The system according to claim 2, wherein said HSM comprises first diversification means using said random number to diversify said master key replacement key data block, which generates a unique key replacement key associated with said non-mutable unique identification number.

5. The system according to claim 3, wherein said HSM comprises encrypting means for encrypting said random number using said at least one stored public key, which generates a unique cryptogram associated with said non-mutable unique identification number.

6. The system according to claim 5, wherein said unique cryptogram is stored on said first server.

7. The system according to claim 2, wherein said random number is deleted inside said first HSM.

8. The system according to claim 3, comprising first transfer means for transferring to said PSD writer and injecting into said at least one PSD said unique key replacement key.

9. The system according to claim 8, wherein said unique key replacement key is registered with said security executive and installed in said first high level key slot.

10. The system according to claim 9, wherein said unique key replacement key is registered with said security executive and installed in said second high level key slot.

11. The system according to claim 2, wherein said HSM comprises second diversification means using said unique identification number to diversify said at least one stored master key data block, which generates a unique master key.

12. The system according to claim 11, comprising second transfer means for transferring to said PSD writer and injecting into said at least one PSD said unique master key.

13. The system according to claim 12, wherein said unique master key is registered with said security executive and installed in said second high level key slot.

14. The system according to claim 13, wherein said unique master key is registered with said security executive and installed in said first high level key slot.

15. A data processing system for post issuance master key replacement for at least one personal security device PSD, said system comprising:

a client functionally connected to said at least one PSD and in secure communications with a first server;

said at least one PSD including a non-mutable unique identification number, a pre-installed key replacement key, an active master key and a security executive, wherein said PSD is functionally connected to said client;

a first server including at least one stored unique cryptogram associated with said non-mutable unique identification number, wherein said first server is functionally connected to a first hardware security module HSM and in secure communications with said client;

a second server functionally connected to a second HSM;

said first HSM including cryptography means, key generation and key transfer means, wherein said first HSM is functionally connected to said first server;

said second HSM including cryptography means, a master key replacement key data block, a master key data block, key generation and key transfer means, at least one stored private key, wherein said second HSM is functionally connected to said second server.

16. The system according to claim 15, comprising first transfer means for securely transferring said master key replacement key data block, said master key data block, and said at least one stored private key from said second HSM to said first HSM.

17. The system according to claim 15, comprising second transfer means for transferring said non-mutable unique identification number to said first server and retrieving means for retrieving said at least one stored unique cryptogram corresponding to said non-mutable unique identification number.

18. The system according to claim 17, comprising third transfer means for transferring said at least one stored unique cryptogram and said non-mutable unique identification number from said first server to said first HSM.

19. The system according to claim 18, comprising decrypting means using said at least one stored private key to decrypt said at least one stored unique cryptogram, resulting in a random number specific to said at least one PSD.

20. The system according to claim 19, comprising first diversification means using said random number to diversify said master key replacement key data block, generating a master key replacement key specific to said at least one PSD.

21. The system according to claim 18, comprising second diversification means using said non-mutable unique identification number to diversify said master key data block, generating a new master key specific to said at least one PSD.

22. The system according to claim 20, comprising fourth transfer means for securely transferring said master key replacement key to said PSD and said security executive comprises comparison means for comparing said master key replacement key to said pre-installed key replacement key.

23. The system according to claim 22, comprising unlocking means for unlocking said security executive upon a match between said master key replacement key and said pre-installed key replacement key.

24. The system according to claim 23, wherein said active master key is deleted from said at least one PSD.

25. The system according to claim 24, comprising means for securely transferring, installing inside said at least one PSD and registering with said security executive said new master key.

26. The system according to claim 25, comprising means for relocking said security executive following installation of said new master key.

27. The system according to claim 16, wherein said secure transfer occurs at said second server.

28. The system according to claim 27, wherein said secure transfer occurs at said first server.

29. A method for initially generating and installing a master key replacement key and a master key for at least one personal security device PSD, said method comprising:

receiving a unique PSD identification number by a first data processing device,

generating a master key data block, a master key replacement key data block and asymmetric key pair by a second data processing device,

transferring said master key data block, said master key replacement key data block and a public key of said asymmetric key pair from said second data processing device to said first data processing device,

generating a random number by said first data processing device,

diversifying said master key replacement data block using said random number and generating a replacement key by said first data processing device,

encrypting said random number with said public key, forming a cryptogram by said first data processing device,

associating said cryptogram with said unique PSD identification number by said first data processing device,

storing said cryptogram by said first data processing device,

deleting said random number from said first data processing device,

diversifying said master key data block using said unique PSD identification number and generating a master key by said first data processing device,

operatively installing said master key replacement key and said master key inside said at least one PSD by said first data processing device.

30. The method according to claim 29, wherein said first data processing device is an access server.

31. The method according to claim 30, wherein said first data processing device is a first hardware security module HSM functionally connected to said access server.

32. The method according to claim 29, wherein said second data processing device is a key management server.

33. The method according to claim 32, wherein said second data processing device is a second hardware security module HSM functionally connected to said key management server.

34. The method according to claim 33, wherein said second data processing device is said second HSM functionally connected to said access server.

35. A method for post issuance master key replacement for at least one personal security device PSD, said method comprising:

receiving a unique PSD identification number by a first data processing device,

generating a new master key data block, a master key replacement key data block by a second data processing device,

transferring said new master key data block, said master key replacement key data block and a private key from said second data processing device to said first data processing device,

cross-referencing said unique PSD identification number with a stored cryptogram associated with said at least one PSD by said first data processing device,

retrieving and decrypting said cross-referenced cryptogram using said private key, forming a random number,

diversifying said master key replacement data block using said random number and generating a master key replacement key by said first data processing device,

diversifying said master key data block using said unique PSD identification number and generating a new master key by said first data processing device,

establishing a secure channel with said at least one PSD by said first data processing device,

unlocking a security executive associated with said at least one PSD, using said master key replacement key by said first data processing device,

deleting an existing master key by said first data processing device,

installing said new master key by said first data processing device,

relocking said security executive by said first data processing device,

releasing said secure channel to said at least one PSD by said first data processing device.

36. The method according to claim 35, wherein said first data processing device is an access server.

37. The method according to claim 36, wherein said first data processing device is a first hardware security module HSM functionally connected to said access server.

38. The method according to claim 35, wherein said second data processing device is a key management server.

39. The method according to claim 38, wherein said second data processing device is a second hardware security module HSM functionally connected to said key management server.

40. The method according to claim 39, wherein said second data processing device is said second HSM functionally connected to said access server.